Notice of Allowability	Application No.	Applicant(s)	
	10/075,016	ASANO, TOMOYUKI	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *interview on 4/10/2006*.

2. ☒ The allowed claim(s) is/are *1-46*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

CHRISTOPHER REVAK
PRIMARY EXAMINER

Cel 4/26/06

DETAILED ACTION

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Bruno Polito (Reg. No. 38,580) on 4/10/2006.

This application has been amended as follows:

IN THE CLAIMS

Replace claims 1, 6, 12, 16, 21, 23, 24, 25, 35, 44 and 46 as follows.

Claim 1: An information playback device for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the information playback device comprising:

a cryptosystem unit operable to determine the validity of a public key certificate of the content recording entity, to acquire a public key of the content recording entity from the public key certificate if the public key certificate is valid,

and to decrypt the encrypted content if the validity of a digital signature of the content recording entity is verified based on the acquired public key;

whereby the device corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by a ~~the~~ device of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to an inhibited ~~the~~ device and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by ~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the inhibited device's leaf key.

Claim 6: An information recording device for recording information on a recording medium, the information recording device comprising:

a cryptosystem unit operable to encrypt content recorded on the recording medium by a content recording entity, to generate a digital signature of the content recording entity, and to record the encrypted content, the digital signature, and

a public key certificate of the content recording entity on the recording medium so as to correspond to one another;

whereby the recording medium is operable with a device that corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by a ~~said~~ device of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to an inhibited ~~said~~ device and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by ~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the inhibited device's leaf key.

Claim 12: A method for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the method comprising:

determining the validity of a public key certificate of the content recording entity;

acquiring a public key of the content recording entity from the public key certificate if the public key certificate is valid;

verifying the validity of a digital signature of the content recording entity based on the acquired public key; and

decrypting the encrypted content if the validity of the digital signature is verified;

whereby the method is implemented on a device for playing back information from the recording medium and the device corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by a ~~said~~ device of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to an inhibited ~~said~~ device and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by ~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the inhibited device's leaf key.

Claim 16: A method for recording information on a recording medium, comprising:

encrypting content recorded on the recording medium by a content recording entity;

generating a digital signature of the content recording entity; and

recording the encrypted content, the digital signature, and a public key certificate of the content recording entity on the recording medium so as to correspond to one another;

whereby the recording medium is operable with a device that corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by a ~~said~~ device of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to an inhibited ~~said~~ device and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by

~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the inhibited device's leaf key.

Claim 21: A computer-readable medium, comprising:

encrypted content recorded thereon by a content recording entity;

identification data for identifying the content recording entity;

a public key certificate of the content recording entity; and

a digital signature of the content recording entity;

whereby the medium is operable with a device that corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by a ~~said~~ device of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to an inhibited ~~said~~ device and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the

lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by ~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the inhibited device's leaf key.

Claim 23: A program storage medium storing a computer program for controlling a computer system to execute a process for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the computer program comprising:

determining the validity of a public key certificate of the content recording entity;

acquiring a public key of the content recording entity from the public key certificate if the public key certificate is valid;

verifying the validity of a digital signature of the content recording entity based on the acquired public key; and

decrypting the encrypted content if the validity of the digital signature is verified;

whereby the computer system corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by the computer system of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to the computer system and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by ~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the computer system's leaf key.

Claim 24: A program storage medium storing a computer program for controlling a computer system to execute a process for recording information on a recording medium, the computer program comprising:

encrypting content recorded on the recording medium by a content recording entity;

generating a digital signature of the content recording entity; and

recording the encrypted content, the digital signature, and a public key certificate of the content recording entity on the recording medium so as to correspond to one another;

whereby the recording medium is operable with a device that corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by a ~~said~~ device of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to an inhibited ~~said~~ device and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by ~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the inhibited device's leaf key.

Claim 25: An information playback device for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the information playback device comprising:

a cryptosystem unit operable to acquire from the recording medium identification data representing the content recording entity, to determine a revocation state of the content recording entity based on the acquired identification data, and to decrypt the encrypted content if the content recording entity has not been revoked;

whereby the device corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by a ~~the~~ device of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to an inhibited ~~the~~ device and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by ~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the inhibited device's leaf key.

Claim 35: A method for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the method comprising:

acquiring from the recording medium identification data representing the content recording entity;

determining a revocation state of the content recording entity based on the acquired identification data; and

decrypting the encrypted content if the content recording entity has not been revoked;

whereby the method is implemented on a device for playing back information from the recording medium and said device corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by a ~~said~~ device of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to an inhibited ~~said~~ device and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by ~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the inhibited device's leaf key.

Claim 44: A computer-readable medium, comprising:

encrypted content recorded thereon by a content recording entity;

a public key certificate for the content recording entity;

a digital signature of the content recording entity; and

a revocation list;

whereby the medium is operable with a device that corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by a ~~said~~ device of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to an inhibited ~~said~~ device and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by ~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the inhibited device's leaf key.

Claim 46: A program storage medium storing a computer program for controlling a computer system to execute a process for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the computer program comprising:

acquiring from the recording medium identification data representing the content recording entity;

determining a revocation state of the content recording entity based on the acquired identification data; and

decrypting the encrypted content if the content recording entity has not been revoked;

whereby the computer system corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and

whereby decryption by the computer system of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to the computer system and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by ~~and encrypting the lowest-level changed key according to~~ a device leaf key other than the computer system's leaf key.

Allowable Subject Matter

1. Claims 1 – 46 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claims 1, 6, 12, 16, 21, 23, 24, 25, 35, 44 and 46.

The prior arts Ginter in combination with Ober, fail to teach or suggest a information playback device, wherein the device corresponds to a leaf of a key-tree structure, said key-tree structure including a plurality of nodes and a plurality of leaves, said plurality of nodes including a root node, and each of said nodes and each of said leaves corresponding to a respective encryption key; and the decryption by a device of said encrypted content is selectively inhibited by changing all keys corresponding to nodes included in a node path between said leaf corresponding to an inhibited device and said root node to generate a plurality of changed keys, said changed keys being propagated through said key-tree structure by encrypting each changed key according to a lower-level changed key, wherein the lowest level node of the key-tree structure to which a changed key is assigned has its said assigned changed key encrypted by a device leaf key other than the inhibited device's leaf key.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

CHRISTOPHER REVAK
PRIMARY EXAMINER
Cel 4/26/06